

REMOTE AUTHENTICATION SYSTEM

Publication number: JP11224236 (A)

Publication date: 1999-08-17

Inventor(s): NAKAMURA HIROSHI; FUJII TERUKO; SADAKANE TETSUO;
BABA YOSHIMASA +

Applicant(s): MITSUBISHI ELECTRIC CORP +

Classification:





- international: G06F12/14; G06F21/20; G06F21/24; G07C9/00; H04L9/32;
G06F12/14; G06F21/00; G06F21/20; G07C9/00; H04L9/32;
(IPC1-7): G06F15/00; H04L9/32

- European: G07C9/00B6D4

Application number: JP19980024225 19980205

Priority number(s): JP19980024225 19980205

Also published as:

 EP0935221 (A2)
 EP0935221 (A3)
 EP0935221 (B1)
 DE69832145 (T2)

Abstract of JP 11224236 (A)

PROBLEM TO BE SOLVED: To provide a remote authentication system capable of surely judging the identification an individual and the presence/absence of his access right and substantially improving handleability at the time of authenticating the individual by using obtained biometrics information and key inputted user identification information corresponding to the operation of a prescribed authentication information acquisition software. SOLUTION: In a Web system 1, authentication is performed by biometrics information. In this case, corresponding to an accessing user terminal 5, a data kind as access information, an authentication request part 4B operated in a Web server terminal 4 as a client of the authentication, the environment of a Web server S/W4C being an application in use and authentication history (authentication time state), an authentication information obtaining S/W for dynamically obtaining the information required for the authentication is selected. Thus, identification of an individual and the presence/absence of his access right are surely judged corresponding to the environment.



Data supplied from the **espacenet** database — Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-224236

(43) 公開日 平成11年(1999) 8月17日

(51) Int.Cl.⁹

G 0 6 F 15/00

H 0 4 L 9/32

識別記号

3 3 0

F I

C 0 6 F 15/00

H 0 4 L 9/00

3 3 0 F

6 7 3 D

審査請求 未請求 請求項の数 3 O L (全 14 頁)

(21) 出願番号

特願平10-24225

(22) 出願日

平成10年(1998) 2月5日

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 中村 浩

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 藤井 照子

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(72) 発明者 貞包 哲男

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 弁理士 宮田 金雄 (外2名)

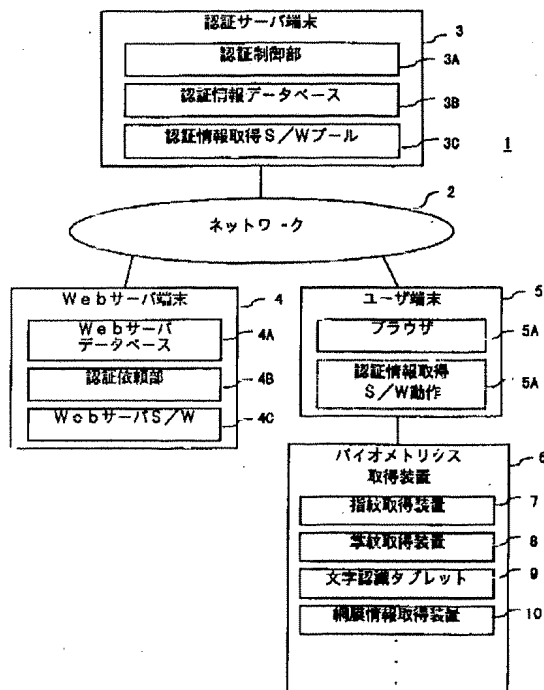
最終頁に続く

(54) 【発明の名称】 遠隔認証システム

(57) 【要約】

【課題】 遠隔認証システムにおいて、バイオメトリクス情報によりユーザの認証を行う際、確実にユーザの特定とアクセス件の有無を判定し得ると共に使い勝手を格段的に向上する。

【解決手段】 ユーザ端末には少なくとも1又は複数種類のバイオメトリクス取得装置が接続され、認証サーバにはユーザ端末及び又はユーザに応じた1又は複数の認証情報取得ソフトウェアが格納され、認証に際して認証サーバからダウンロードされるユーザ端末及び又はユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、1又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにした。



【特許請求の範囲】

【請求項1】 ネットワークに認証サーバと、認証クライアントと、ユーザ端末がそれぞれ接続され、上記ユーザ端末を通じて上記認証クライアントにアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも1又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた1又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記1又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたことを特徴とする遠隔認証システム。

【請求項2】 ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、上記ユーザ端末にアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも1又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた1又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記1又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたことを特徴とする遠隔認証システム。

【請求項3】 上記ユーザ端末に接続された上記複数のバイオメトリクス取得装置のうち、何れかを用いて上記バイオメトリクス情報として入力するかを上記ユーザが選択する手順を有する認証情報取得ソフトウェアを備えることを特徴とする請求項1又は請求項2に記載の遠隔認証システム。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】この発明は、遠隔認証システムにおいて、バイオメトリクスにより個人の特定とその個人の情報やアプリケーションへのアクセス権の有無の判定を1つの認証サーバ端末にて集中的に行うシステムに関するものである。

【0002】

【従来の技術】従来、ネットワークに接続された情報処理システムにおいて機密保持のため、個人を特定し該個人のアクセス許可と不許可の判断を行う、すなわち認証が必要である。また、銀行の現金自動支払い機等では個人の特定と預金残高等該個人の取り引き情報にアクセスするための認証や、機密度の高い研究場所や会員制クラブ等への入退室時にも個人の認証が実施されている。

【0003】これらの認証として、身分証明書等と同様

の位置づけである磁気カードやICカード、パスワード等の個人の記憶や、これらの組み合わせによって個人の特定と資格の認定、すなわち認証を実施している。ところがパスワード等は忘却の恐れがあり、磁気カードやICカード等は紛失や破壊等により認証が不能に陥ったり、盗難やパスワード情報の漏洩により本人以外が本人と成りすまして認証されてしまう等の問題がある。またこれらによって機密度を高く保つためには、確実に本人と認証する必要があるが、パスワード等を複雑にしたリ、ワンタイムパスワード(OTP)等の手段を用いると、その分記憶し難くなったり、認証操作自体が煩雑になる。さらに磁気カード等を使用しないで、記憶による認証を広域で実施(銀行の複数の店舗で使用)する場合には、認証情報は集中的に管理する必要がある。

【0004】

【発明が解決しようとする課題】一方、指紋情報、掌紋情報、筆跡情報、網膜情報等の個人の生体的特徴であるバイオメトリクス情報による認証では、煩雑さを解消すると共に成りすましが困難である。バイオメトリクス情報による認証が広域で必要な場合には、上述と同様の理由及びプライバシー保護の面からも、集中的な管理と認証が必要である。このバイオメトリクス情報による認証を集中的に実施する場合、ユーザ毎だけではなく、認証を必要とするものや場所、システム等のセキュリティレベル(機密レベル)により適切な認証方法を選択して、認証情報を取得することが重要である。

【0005】ここでIETF(Internet Engineering Task Force)のRFC(Request For Comment)に登録されているRFC2138(Remote Authentication Dial In User Service、以下RADIUS、前RFC2058が更新)で記述されているRADIUSサーバは、RADIUSクライアントの認証要求を受け集中的に認証処理を行い認証結果を返送するが、認証手段や認証情報はユーザ毎に固定的に予め決められており、バイオメトリクス情報を取得する場合にはその取得環境に応じて動的に認証手段と認証情報を変更できないという問題があった。

【0006】このような従来例として、さらに特開平9-81518号公報に示される「ネットワーク上の認証方法」のように、ユーザホストがアプリケーションサーバにアクセスしてきた場合に、アプリケーションサーバが認証サーバに固定的な認証手段と認証情報を使用してユーザの認証を依頼し、認証結果を受けるような認証方法がある。

【0007】またバイオメトリクス情報は個人を識別するのに有効であるが、プライバシー保護の問題と、バイオメトリクス取得装置自体が不潔なものや不快を伴う場合のように衛生的に取得上の問題もある。

【0008】この発明は以上の問題点を解消するためなされたもので、バイオメトリクス情報により個人の認証を行う際、確実に個人の特定と該個人のアクセス権の有

無を判定し得ると共に使い勝手を格段的に向上し得る遠隔認証システム及び遠隔認証方法を得ることを目的とする。

【0009】

【課題を解決するための手段】この発明に係る遠隔認証システムは、ネットワークに認証サーバと、認証クライアントと、ユーザ端末がそれぞれ接続され、上記ユーザ端末を通じて上記認証クライアントにアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも1又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた1又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記1又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたものである。

【0010】また次の発明に係る遠隔認証システムは、ネットワークに認証サーバと、ユーザ端末がそれぞれ接続され、上記ユーザ端末にアクセスするユーザの認証を行う遠隔認証システムにおいて、上記ユーザ端末には少なくとも1又は複数種類のバイオメトリクス取得装置が接続され、上記認証サーバには上記ユーザ端末及び又は上記ユーザに応じた1又は複数の認証情報取得ソフトウェアが格納され、認証に際して上記認証サーバからダウンロードされる上記ユーザ端末及び又は上記ユーザに応じた所定の認証情報取得ソフトウェアの動作に応じて、上記1又は複数種類のバイオメトリクス取得装置で取得されたバイオメトリクス情報及び又はキー入力されたユーザ識別情報を用いるようにしたものである。

【0011】さらに次の発明に係る遠隔認証システムは、上記ユーザ端末に接続された上記複数のバイオメトリクス取得装置のうち、何れかを用いて上記バイオメトリクス情報として入力するかを上記ユーザが選択する手順を有する認証情報取得ソフトウェアを備えるものである。

【0012】

【発明の実施の形態】以下図面を参照して、この発明の実施の形態について詳述する。

【0013】実施の形態1. 図1にこの発明をWebシステム1に適用した場合の実施の形態1の構成を示す。ネットワーク2上に認証サーバ端末3、認証クライアント端末4（本例ではWebサーバ端末）、ユーザ端末5等が接続される。このようなWebシステム1でWebサーバ4はユーザからユーザ端末5を通じてアクセスされた時に、そのユーザの個人認証を認証サーバ端末3から受け、その結果によりユーザに対してサービスを行う。

【0014】認証サーバ端末3は、認証制御部3Aと、認証情報データベース3Bと、認証情報取得ソフトウェア（以下、ソフトウェアは、S/Wと記述する）3Cとを格納するパーソナルコンピュータやワークステーション等のコンピュータ装置（以下、構成としてCPU、メモリ、ディスク、通信制御部等を有するものを示す）である。またWebサーバ端末4は、Webサーバデータベース4Aと、認証依頼部4B及びユーザの認証に必要なWebサーバS/W4Cが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。

【0015】ユーザ端末装置5は、Webサーバ端末4の情報を表示するブラウザ5Aと、認証情報取得S/W5Bが動作するパーソナルコンピュータやワークステーション等のコンピュータ装置である。またユーザ端末装置5にはバイオメトリクス取得装置6が接続されている。バイオメトリクス取得装置6は、画像処理等により人体の指紋や掌紋情報をバイオメトリクス情報として取得する指紋取得装置7や掌紋取得装置8、ユーザが描いた筆跡情報をバイオメトリクス情報として取得する文字認識タブレット9、眼底スキャン等によって人体の網膜情報をバイオメトリクス情報として取得する網膜情報取得装置10等を示している。

【0016】このようなWebシステム1における認証処理の流れを図2に示す。まずユーザ端末装置5で動作しているアプリケーションであるブラウザ5Aにより、ユーザが認証のクライアントであるWebサーバ端末4の機密度の高いWebサーバデータベース4Aの情報にアクセスした場合（SP1）について説明する。その機密度の高い情報のアクセス制御を行っているアプリケーションであるWebサーバS/W4Cは、該ユーザがアクセス権限を有すか否かの判定するためにユーザ認証を行う必要がある（SP10）。

【0017】すなわちWebサーバ端末4のWebサーバS/W4Cは、クライアントID（認証依頼部の識別子）、アプリケーションID（認証を必要とするアプリケーションであるWebサーバS/W4Cの識別子）、アクセスデータ種別（ユーザがアクセスしてきたデータの機密レベル）と共に認証依頼部4Bにユーザの認証が必要であることを通知する（SP11）。認証依頼部4Bは認証サーバ端末3へ上記情報を含むユーザの認証要求を送信する。

【0018】ユーザの認証要求を受信した認証サーバ端末3の認証制御部3Aは認証クライアントID、アプリケーションID、アクセスデータ種別から、認証情報取得S/W11を選択する（SP20）。認証情報取得S/W11はそれぞれ取得する認証情報が決まっており、複数の認証情報を取得する認証情報取得S/W11もある。認証制御部3Aは選択した認証情報取得S/W11を認証のクライアントであるWebサーバ端末4へ転送

する（SP21）。

【0019】Webサーバ端末4の認証依頼部4Bは、WebサーバS/W4Cに転送された認証情報取得S/W11を引き渡し、ユーザから認証情報の取得を指示し、その指示によりWebサーバS/W4Cからユーザ端末5に認証情報取得S/W11が転送される（SP12）。

【0020】ユーザ端末5のブラウザ5Aは転送された認証情報取得S/W11を受け取り、この認証情報取得S/W11を認証情報S/W5Bとして動作させる（SP2）。認証情報S/Wは、自発的にユーザID（名前、会社、社員番号、所属、住所、電話等や、システムで個人毎に割り振られているID）の取得と、指紋情報、掌紋情報、筆跡情報、網膜情報等のバイオメトリクス情報や、パスワードやワンタイムパスワード等の従来のコンピュータシステムで通常使用される認証情報を取得する。このとき認証情報を取得するドライバ等の他のS/Wと協調して動作する場合もある。認証情報取得S/W5Bは、ブラウザ5Aを介してWebサーバ端末へ取得したユーザIDと認証情報を転送する（SP3）。

【0021】Webサーバ端末4の認証依頼部4BはWebサーバS/W4Cを介して、ユーザから取得したユーザIDと認証情報を認証サーバ端末3へ転送する（SP13）。認証サーバ端末3の認証制御部3Aは転送されたユーザIDと認証情報により、ユーザ認証を実施する（SP22）。このとき転送されたバイオメトリクス情報等の認証情報は、認証サーバ端末3の認証情報データベース3Bに元々蓄積されている個人情報と照合する。転送された全ての認証情報の照合で本人と判断した場合には、この結果を認証のクライアントであるWebサーバ端末に通知する。また、照合結果が1つでも正しくなければ本人ではないと判断しこれを通知する（SP23）。

【0022】認証結果を受けた認証のクライアントであるWebサーバ端末4の認証依頼部4Bは、その認証結果をWebサーバS/W4Cに通知する。WebサーバS/W4Cは該認証結果により該ユーザに対してWebサーバデータベースの機密度の高い情報へのアクセス許可又は不許可を判定する（SP14）。例えば、該機密情報の表示を行う等、ユーザアクセスに対する動作を行う。

【0023】なおユーザ端末5（認証情報取得S/W5B）とWebサーバ端末4間と、Webサーバ端末4と認証サーバ端末3間（認証制御部3A）は暗号化すれば認証情報の秘匿を行えると共に、成りすましの脅威を減ずることができる。また個別端末間ではなく、ユーザ端末5（認証情報取得S/W5B）と認証サーバ端末3間（認証制御部3A）で暗号化を実施しても同様に成りすましの脅威を減ずることができる。

【0024】実施例1．ここで図3、図4を用いて、データベース構造の単純な例と認証情報取得S/W5Bの選択処理について説明する。図3の認証情報データベース3Bには個人ユーザ毎の情報として、ユーザID、ユーザレベル、認証情報の項目が格納されている。ユーザIDは、名前、会社、社員番号、所属、住所、電話等や、システムで個人毎に割り振られているIDである。またユーザレベルは機密情報へのアクセスレベルであり、さらに認証情報は照合元の認証情報としての指紋情報、筆跡情報、網膜情報等のバイオメトリクス情報、パスワード情報やワンタイムパスワードの情報等である。

【0025】図4の認証情報取得S/Wプール3Cには、指紋情報と網膜情報の両方を取得する認証情報取得S/W11や、2本の指紋情報を取得する認証情報取得S/W11、指紋情報と筆跡情報を取得する認証情報取得S/W11等が格納されている。また、認証情報取得S/Wプール3Cは、機密レベルに対応した選択可能な認証情報取得S/W11とデータ種別が示されている。

【0026】この実施例1での認証サーバ端末3の認証情報取得S/W11の選択機構の説明として、まずデータ種別=17のWebサーバデータベース4Cの情報にユーザがアクセスしてきた場合を例とする。このとき認証依頼部4Bの識別子に相当する認証クライアントID=15とし、WebサーバS/W4Cの識別子に相当するアプリケーションID=25とする。WebサーバS/W4Cはデータ種別=17にアクセス発生時、認証依頼部4Bにユーザの認証が必要であることを通知する。認証依頼部4Bは認証サーバ端末3へ上記情報、データ種別=17、認証クライアントID=15、アプリケーションID=25を含むユーザの認証要求を送信する。そしてこれらの情報を含んだ認証要求を認証サーバ端末3が受信する。

【0027】認証サーバ端末3の認証制御部3Aは、図4の認証情報取得S/Wプール3Cのデータベースと受信した認証要求のデータ種別から要求されたデータは機密度レベル2であるため、図示のようにレベル2以上の認証情報取得S/W11の選択可能候補を知る。

【0028】実施例2．また図5及び図6を用いて、図3と同様に認証情報データベースの一部の別の実施例を説明する。ここには、認証クライアントID毎やアプリケーションID毎の選択可能な認証情報取得S/W11が示されている。認証サーバ端末3の認証制御部3Aは、これらの情報により、認証クライアントIDから選択できかつアプリケーションIDから選択できる認証情報取得S/W11の候補を知る。従って、データ種別によって、A、B、C、D、E、Fが候補になり、認証クライアントIDによって、C、D、Eが候補になり、アプリケーションIDによって、A、D、E、Fが候補になり、最終的にD、Eのどちらかが選択される。

【0029】この選択可能認証情報取得S/Wの候補が

らの認証サーバ端末3がランダムに選択、または固定的に決まったS/Wを選択、または順次選択といった手段で選択する。この例のように、アクセス情報であるデータ種別や、認証のクライアントである装置で動作している認証依頼部4Bや、使用アプリケーションであるWebサーバS/W4C等の環境に応じて認証手段と認証情報をフレキシブルに選択でき、個人の特定と該個人のアクセス権の有無を環境に応じて確実に判定できる。

【0030】実施例3. 次の実施例として、ユーザIDが認証要求に含まれており、図3の認証情報データベースが図7に示すように詳細設定されている場合を説明する。この処理の流れを図2との対応部分に同一符号を付した図8に示す。まず、Webサーバ端末4は、ユーザID（名前、会社、社員番号、所属、住所、電話等やシステムで個人毎に割り振られているID）を取得し、取得したユーザID、クライアントID（認証依頼部4Bの識別子）、アプリケーションID（認証を必要とするアプリケーションであるWebサーバS/W4Cの識別子）、アクセスデータ種別（ユーザがアクセスしてきたデータの機密レベル）とともに認証依頼部4Bに該ユーザの認証を依頼する。

【0031】図7の認証情報データベース3Bは、ユーザの種別（データ管理者か一般ユーザか等）、使用できる認証クライアントID、使用できるアプリケーションID、本人と認証された場合にアプリケーションに引き渡されるアプリケーションの制御情報、照合ログとして過去の規定認証回数までの認証情報取得S/Wの選択状況と照合率、総認証回数、選択基準等、ユーザ個人毎の情報が図3の認証情報データベースに追加されている。

【0032】ユーザIDが認証要求に含まれている場合には、図7の該当ユーザの選択基準に従って選択する。具体例としてユーザID=1であり、他は前の例と同様にデータ種別=17、認証クライアントID=15、アプリケーションID=25の場合、認証依頼部4Bは認証サーバ端末3へ、上記情報としてユーザID=1、データ種別=17、認証クライアントID=15、アプリケーションID=25を含むユーザの認証要求を送信する。

【0033】そしてこれらの情報を含んだ認証要求を認証サーバ端末3が受信する。上述と同様にデータ種別によってA、B、C、D、E、Fが候補になり、認証クライアントIDによってC、D、Eが候補になり、アプリケーションIDによってA、D、E、Fが候補になり、最終的にD、Eのどちらかが選択される。また、ユーザID=1であることから、認証制御部3Aは総認証回数によって選択を実施する。総認証回数の1回目はD、2回目はE 3回目はD、4回目E……というように選択する。ここではユーザID=1の総認証回数=20で、今回は21回目であるため認証情報取得S/W11のDが選択される。

【0034】他の実施例。また、図7に示すように認証

情報データベース3Bにユーザ毎に使用できる認証クライアントID、使用できるアプリケーションIDに指定があれば、指定された認証クライアントやアプリケーションを使用しているときのみ該ユーザに対して認証情報取得S/W11を送付する等のアクセス制御が実現できる。ここでは、使用できるクライアントIDに15があり、使用できるアプリケーションIDにも25があるため、認証情報取得S/W11の送付が許可される。

【0035】また、図7に示すユーザ種別によっても認証情報取得S/W11の送付の可否を判定できる。さらに認証クライアントやアプリケーションにユーザと同様に機密レベルを割り振れば、認証情報取得S/W11の選択時に、認証サーバ端末3は認証クライアントのレベルとアプリケーションのレベルとアクセスデータ種別のレベルから認証情報取得S/W11を選択できる。すなわち、例えば3つの中の最も高いレベル以上の認証情報取得S/W11から選択するような制御ができる。

【0036】認証情報取得S/W11の送付以降は、上述と同様であるが、ユーザIDはすでに取得しているため、認証情報のみが転送されるところが異なる。また、図7の本人と認証された場合にアプリケーションに引き渡されるアプリケーションの制御情報である、Key-1をWebサーバ端末4が使用して多彩なアクセス制御を実現することもできる。

【0037】さらに、選択基準が図7の照合率の例として、上述では選択基準が総認証回数であったが、これに代え、選択基準が照合評価とした場合には、レベル2以上の認証情報取得S/W11の中で、過去の照合評価の最も高いものを該ユーザの照合ログから探し、それを選択する。ここでは前回のEの照合評価が最も高いのでEが選択される。

【0038】また、認証サーバ端末3から認証クライアントへの認証取得S/W転送を省略する例もある。上述したWebシステム1のケースでは認証クライアントであるWebサーバ端末4によって、認証情報取得S/Wが固定的に決まってしまう場合には、認証クライアントのWebサーバ端末4が認証情報取得S/W11を予め取得しておき、その認証情報取得S/W11を認証サーバ端末3から認証クライアントのWebサーバ端末4へ、認証情報取得S/Wの転送なしにユーザ端末5に転送するようにしても良い。

【0039】以上のように、このWebシステム1においては、バイオメトリクス情報により認証を行う場合に、アクセスしてきたユーザや、アクセス情報であるデータ種別や、認証のクライアントであるWebサーバ端末4で動作している認証依頼部4Bや、使用アプリケーションであるWebサーバS/W4C等の環境や認証履歴（認証時状態）に応じて、動的に認証に必要な情報を取得する認証情報取得S/W11を選択することにより、個人の特定と該個人のアクセス権の有無をその環境

に応じて確実に判定できる。

【0040】実施の形態2. この実施の形態2においては実施の形態1を簡略化したものである。図1との対応部分に同一符号を付した図9は、バイOMETRICS情報を取得するユーザ端末と認証クライアントの端末が同一である。認証が必要なアプリケーションの例としてデータベース検索を行うデータベース検索アプリケーション5Eがあり、データベース検索アプリケーション5Eが使用するローカルデータベース5C、認証依頼部5D、ユーザの認証が必要なデータベース検索アプリケーション5Eと認証情報取得S/W11が動作するパーソナルコンピュータ、ワークステーション等のコンピュータ装置である。バイOMETRICS取得装置6はユーザ端末5に接続されており、上述した実施の形態1と全く同様の構成であり、また認証サーバ端末3も、上述した実施の形態1と全く同様の構成である。

【0041】基本的には上述の実施の形態1と同じであり、図2、図8との対応部分に同一符号を付した図10において、データベース検索アプリケーション5Eは、ローカルデータベース5Cの機密情報へアクセスする際に(SP5)、まずユーザID(名前、会社、社員番号、所属、住所、電話等や、システムで個人毎に割り振られているID)を取得し(SP6)、取得したユーザID、クライアントID(認証依頼部5Dの識別子)、アプリケーションID(認証を必要とするアプリケーションであるデータベース検索アプリケーション5Eの識別子)、アクセスデータ種別(ユーザがアクセスしてきたデータの機密レベル)と共に、認証依頼部5Dに該ユーザの認証を依頼する(SP7)。

【0042】認証サーバ端末3の動作は実施の形態1と同じであり、認証処理を実行し認証結果を受けた認証のクライアントであるユーザ端末5の認証依頼部5Dは、その認証結果をデータベース検索アプリケーション5Eに通知する。データベース検索アプリケーション5Eは該認証結果により、該ユーザに対してローカルデータベース5Cの機密度の高い情報へのアクセスを許可する可否かを判定する(SP8)。例えば該機密情報の表示を行う等、ユーザアクセスに対する動作を行う。このような構成によれば、ユーザ端末5が認証リクエストを出す構成において、上述した実施の形態1と同一の効果を達成することができる。

【0043】実施の形態3. この実施の形態3では、図2、図8との対応部分に同一符号を付した図11において、認証サーバ3から転送されてきた認証情報取得S/W11が指定する個人認証情報がユーザの意向に合わない場合、ユーザが該認証情報取得S/Wを拒否する手順(SP2B、SP12A)を示す。取得が拒否された認証サーバ端末3は、他の認証情報取得S/Wを再選択する(SP20A)。ただし、図4について上述したように再選択できる認証情報取得S/Wが他にある場合で

ある。

【0044】バイOMETRICSを個人の認証情報として使用する場合には、指定されたバイOMETRICS取得装置6が不潔なものや不快を伴う場合に、ユーザが拒否ができる必要がある。バイOMETRICSは個人を識別するのに有効であるが、プライバシー保護の問題と上記のように衛生上の問題もあるため、ユーザが拒否又は変更できる機会が必須である。

【0045】またバイOMETRICS取得装置6がセキュリティ的に信用できない場合も、バイOMETRICS情報以外の煩雑ではあってもワンタイムパスワード(OTP)等の代替手段を指定したいという意向があり、ユーザの拒否又は変更の意向に従っても、動的に認証に必要な情報を取得する認証情報取得S/Wを選択することにより、個人の特定と該個人のアクセス権の有無をその環境に応じて確実に判定できる効果をえられる。

【0046】実施の形態4. 実施の形態3と同様の効果を得る手段として、実施の形態1、2の認証情報取得S/W自体に取得認証情報の選択機構が含まれる。実施の形態1の例では選択できる認証情報取得S/WにはDの指紋と筆跡情報で認証実施するものと、Eの指紋のみで認証するものが選択できる。このとき認証サーバはDとE両方の認証情報取得機能を兼ね備えた認証情報取得S/Wを転送するところが異なる。

【0047】Webシステム1自体の構成や動作手順は、実施の形態1、2と同様である。ユーザ側での認証情報取得S/Wの画面イメージを図12に示す。ユーザはD/Eからどちらかを選択して、認証手段と自分自身の認証情報の取得を行う。画面の選択ボタン12A、12Bの何れかを選択すると認証情報取得S/Wが動作して、実際に選択された認証情報の取得を行う。認証サーバ端末3では送られてきた認証情報の種別と共に、送られてきた情報の組で認証可能かを判断でき、実施の形態3と同様の効果を得ることができる。

【0048】実施の形態5. 上述の実施の形態1~4では、認証情報取得S/Wによって取得する認証情報が決定されていたが、認証情報取得S/Wではなく画面に取得する認証情報が示されるだけのようにしても良い。例えば実施の形態1の詳細データベースの認証回数の時には、画面に指紋情報と筆跡情報を送るように表示する。これによりユーザは表示された内容に従い自発的に認証情報を取得するソフトウェア等を動作させて、取得した認証情報を認証サーバ3に送る。

【0049】また、表示で具体的に示されず、予め決められた認証情報を送付するよう表示するようによっても良い。この場合はユーザの記憶によって予め事前に別途ユーザに対して、管理者等から通知されている全ての認証情報を、ユーザは自発的に認証情報を取得するソフトウェア等を動作させて、取得した認証情報を認証サーバに送る。このようにすれば上述の実施の形態1と同様の効

果を実現できるが、表示では具体的に示されず予め決められた認証情報を送付する場合に、取得する手段がパスワード的な扱いとなるため、セキュリティを一段と向上できる。

【0050】なお上述の実施の形態1～4においては、Webサーバ端末4において、ユーザの個人認証を行う場合について述べたが、この発明はこれに限らず、例えばネットワークに接続された入退室端末装置等のように、ユーザの個人認証が必要な制御装置一般に広く適用できる。

【0051】

【発明の効果】上述の通りこの発明によれば、認証サーバは、バイオメトリクス情報により認証を行う際に、ユーザのバイオメトリクス情報の取得環境に応じて、バイオメトリクス取得装置と認証情報を自由に選択し取得ができ、かくして確実にユーザの特定とそのユーザのアクセス権の有無を判定し得る遠隔認証システムを実現できる。

【0052】またユーザは指定された認証情報の取得について不満があった場合に、取得する認証情報を変更や拒否することができ、バイオメトリクス取得装置が不潔等で不快感を伴う場合やバイオメトリクス情報を取得する装置が信頼できない場合でも、代替手段で確実にかくして確実にユーザの特定とそのユーザのアクセス権の有無を判定できる。

【図面の簡単な説明】

【図1】 この発明による遠隔認証システムを適用したWebシステムの実施の形態1の構成を示すブロック図である。

【図2】 図1のWebシステムにおける認証処理の説明に供するタイミングチャートである。

【図3】 図1の認証サーバ端末における認証情報データベースの実施例1の説明に供する図表である。

【図4】 図1の認証サーバ端末における認証情報データベースの実施例1の説明に供する図表である。

【図5】 図1の認証サーバ端末における認証情報データベースの実施例2の説明に供する図表である。

【図6】 図1の認証サーバ端末における認証情報データベースの実施例2の説明に供する図表である。

【図7】 図1の認証サーバ端末における認証情報データベースの実施例3の説明に供する図表である。

【図8】 図1のWebシステムにおける実施例3の認証処理の説明に供するタイミングチャートである。

【図9】 この発明による遠隔認証システムを適用したWebシステムの実施の形態2の構成を示すブロック図である。

【図10】 図9のWebシステムにおける認証処理の説明に供するタイミングチャートである。

【図11】 図1のWebシステムにおける認証処理の実施の形態3として拒否が発生した場合の説明に供するタイミングチャートである。

【図12】 図1のWebシステムの実施の形態4として認証情報取得S/Wの表示画面の説明に供する略線図である。

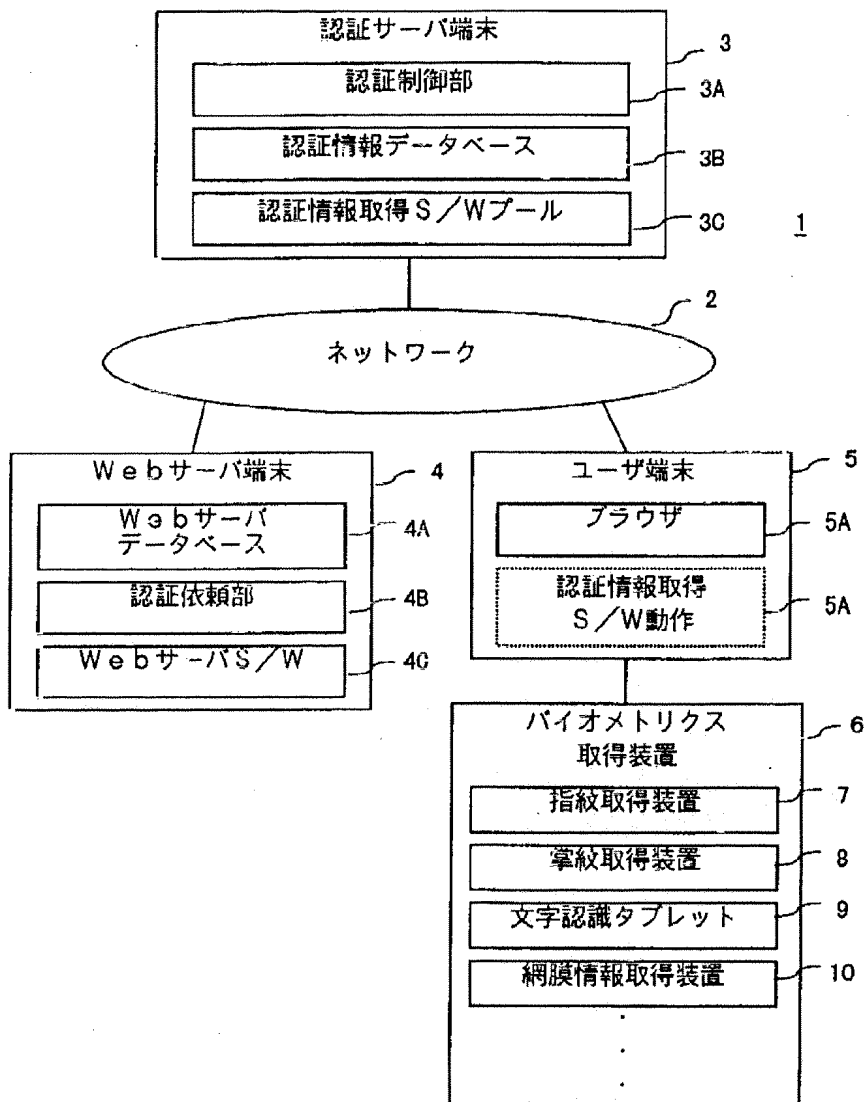
【符号の説明】

- 1 Webシステム
- 2 ネットワーク
- 3 認証サーバ端末
 - 3A 認証制御部
 - 3B 認証情報データベース
 - 3C 認証情報取得ソフトウェアプール
- 4 Webサーバ端末
 - 4A Webサーバデータベース
 - 4B 認証依頼部
 - 4C Webサーバソフトウェア
- 5 ユーザ端末
 - 5A ブラウザ
 - 5B 認証情報取得ソフトウェア動作
- 6 バイオメトリクス取得装置
- 7 指紋取得装置
- 8 掌紋取得装置
- 9 文字認識タブレット
- 10 網膜情報取得装置
- 11 認証情報取得ソフトウェア

【図3】

ユーザID	1 {名前、会社、社員番号、所属、住所、電話、など}	2
ユーザレベル	2			
認証情報	{指紋 1、指紋 2、筆跡、網膜、パスワード、ワンタイムパスワード情報}			

【図1】



【図4】

レベル	データ種別	認証情報取得S/W
1(最高機密)	1~10	A, B, C
2	11~20	D, E, F
3	21~30	G, H

A: 指紋と網膜
 B: 指紋2指
 C: 網膜と筆跡
 D: 指紋と筆跡
 E: 指紋
 F: 筆跡
 G: ワンタイムパスワード
 H: パスワード

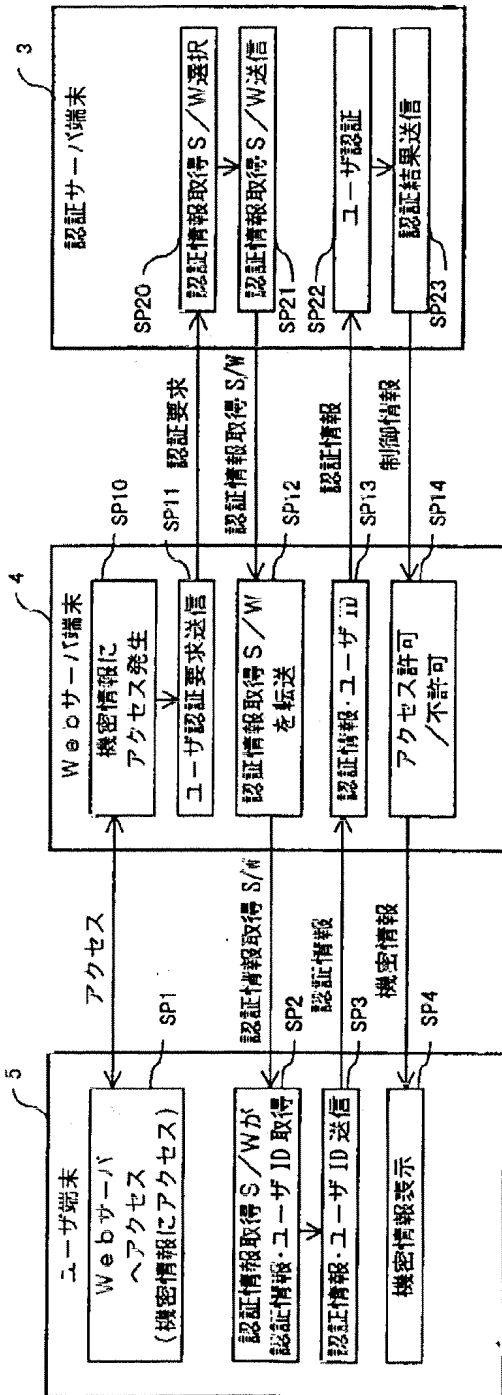
【図5】

認証クライアントID	認証情報取得S/W
	E, F
15	C, D, F
	A, B, C
	D, E, F
	G, H

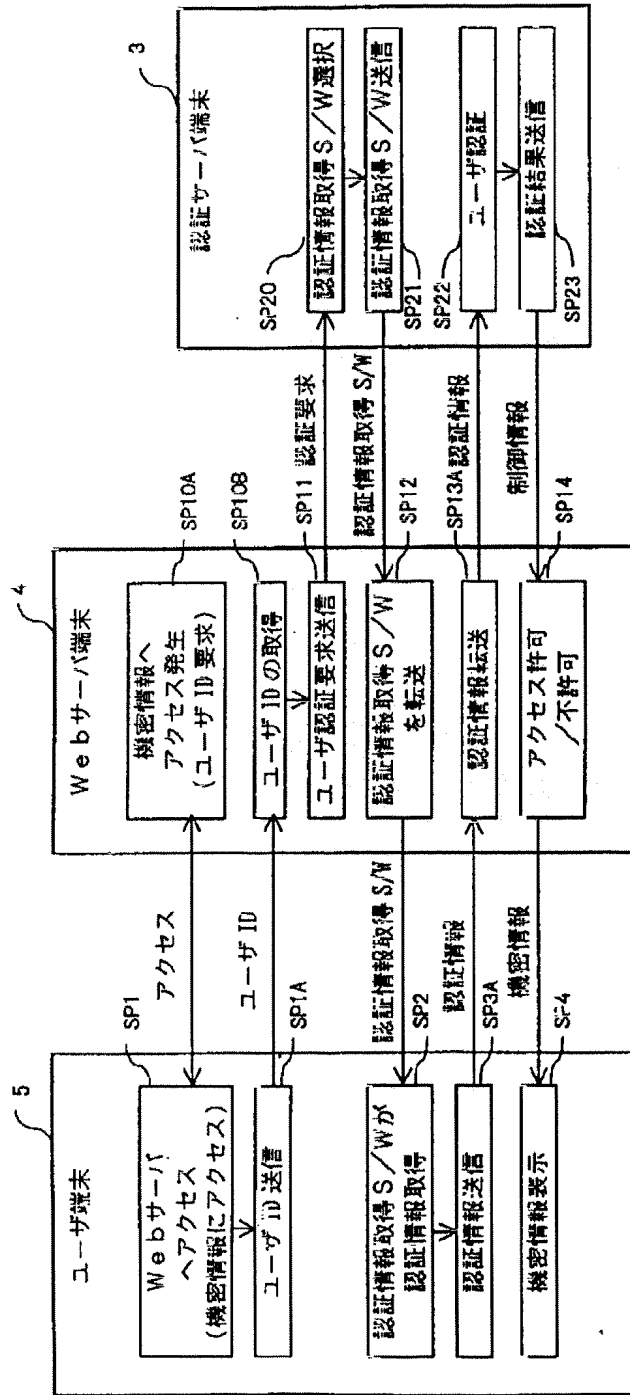
【図6】

アプリケーションID	認証情報取得S/W
	C, D, G
25	A, D, E, F
	E, F
	G, H

【図2】



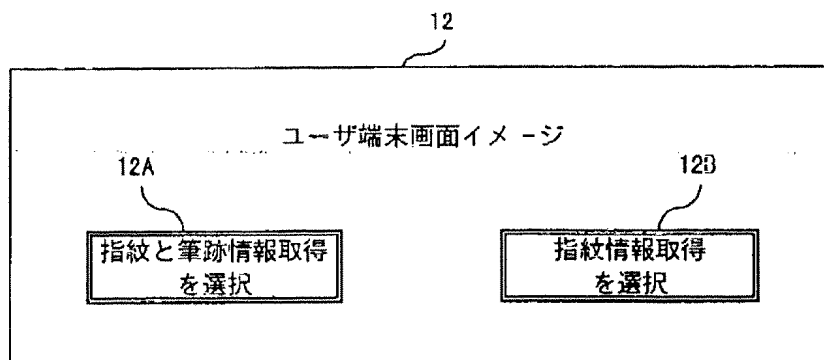
【図8】



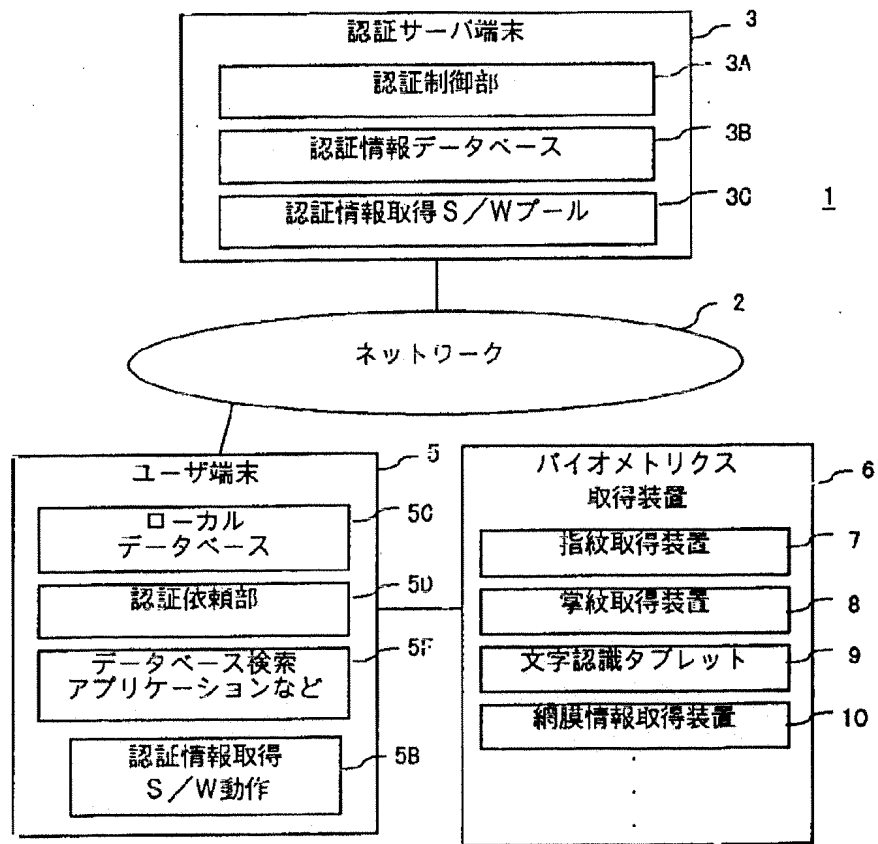
【図7】

ユーザ ID	1 {名前、会社、社員番号、所属、住所、電話、など}	2
ユーザ種別	一般			
ユーザレベル	2			
使用できるクライアント ID	10,15			
使用できるアプリケーション ID	8,25,36			
アプリケーション制御情報	key-1			
認証情報	{指紋1、指紋2、筆跡、網膜、パスワード、ワンタイムパスワード情報}			
照合ログ	前回 : 認証情報取得 S/W E 選択, 照合評価 90%, 指紋 1=90% 前々回 : 認証情報取得 S/W D 選択, 照合評価 75% 指紋 2=80%, 筆跡=70% . . .			
総認証回数	20			
選択基準	総認証回数 (他例: 照合率)	,		

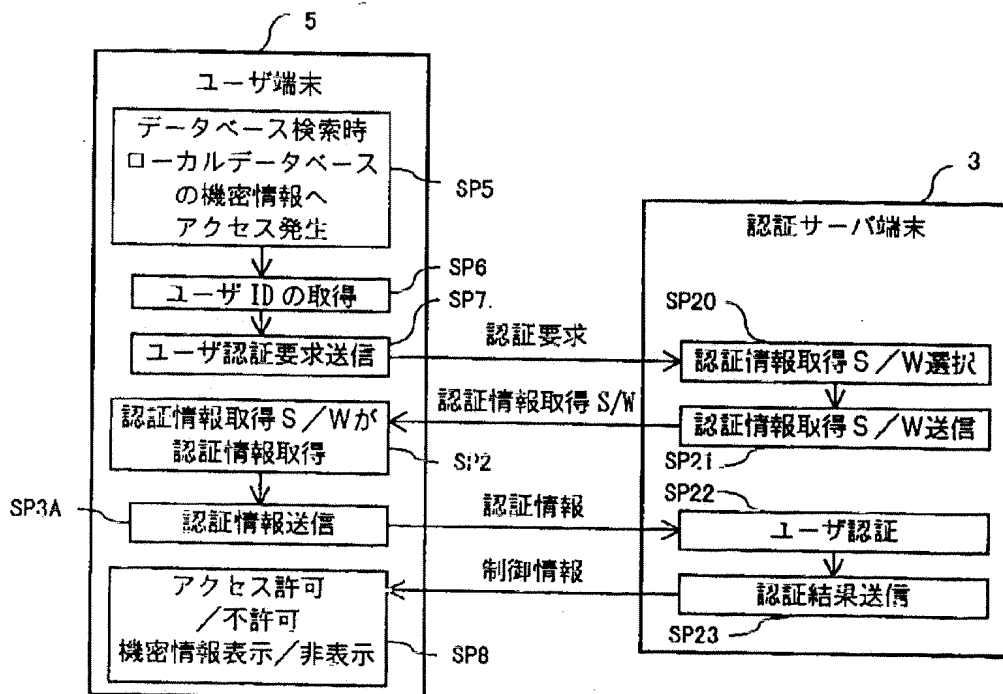
【図12】



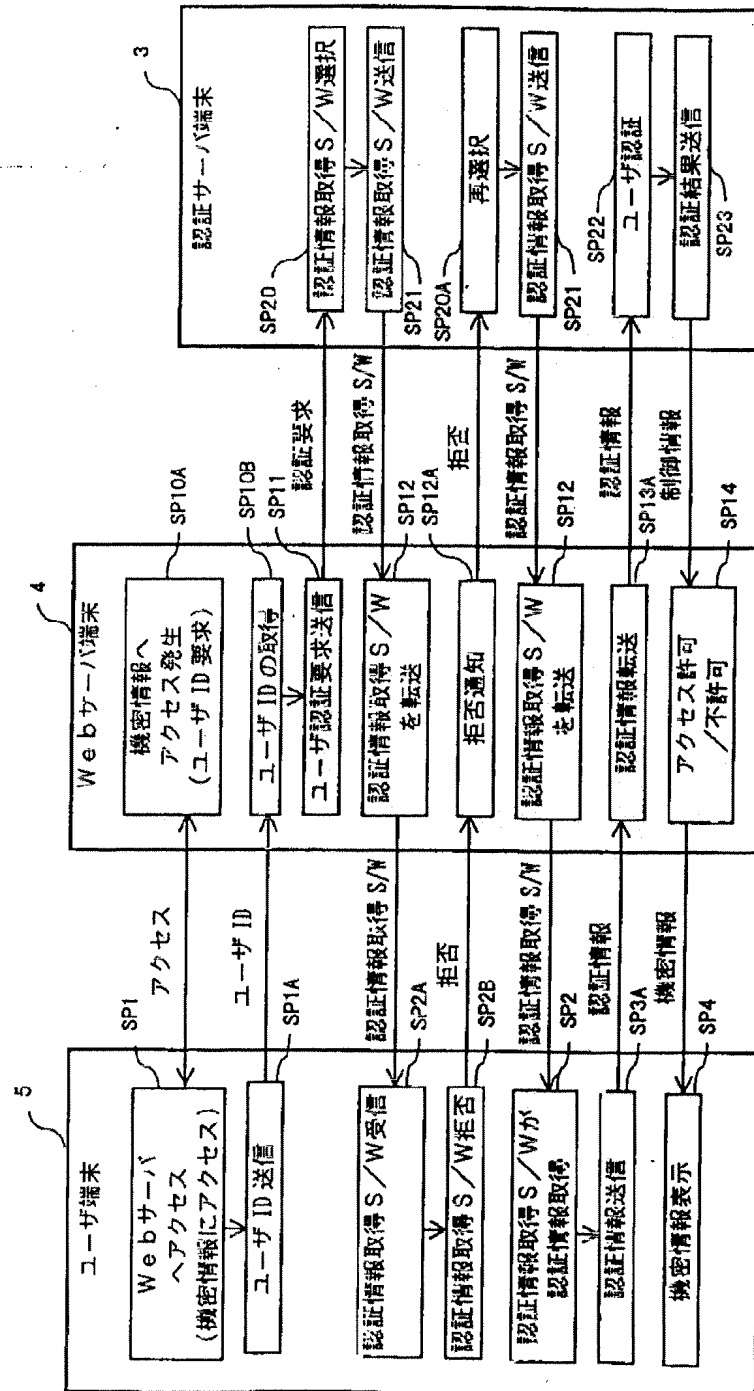
【図9】



【図10】



【図11】



フロントページの続き

(72)発明者 馬場 義昌

東京都千代田区丸の内二丁目 2 番 3 号 三
菱電機株式会社内